TESTIMONY OF DAVID A. WHITELEY
Executive Vice President
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

before the
Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology
Committee on Homeland Security
U.S. House of Representatives
on
"The Cyber Threat to Control Systems: Stronger Regulations are Necessary to Secure the Electric Grid"

October 17, 2007

Mr. Chairman and Members of the Subcommittee, the North American Electric Reliability Corporation[1] ("NERC") is pleased to provide this testimony on how we and the electric industry are working to protect the security of the control systems for the bulk power grid throughout North America pursuant to the authority set forth in Section 215 of the Federal Power Act ("FPA"), as enacted through the Energy Policy Act of 2005 ("EPAct 2005").[2] Protecting the overall reliability of the bulk power system, including ensuring the security and reliability of grid control systems, has been a high priority for NERC since well before the enactment of EPAct 2005, and we take this matter very seriously. As the Committee is aware, under the authority of FPA Section 215, NERC has proposed eight Critical Infrastructure Protection Reliability Standards for approval by the Federal Energy Regulatory Commission ("FERC" or "Commission"). FERC approval of the standards that NERC has proposed in this area, along with parallel action by appropriate governmental authorities in Canada, will enhance the cybersecurity of these control systems and the reliability of the interconnected electric transmission grid.

EXECUTIVE SUMMARY

Cyber security of control systems is an increasing priority for every sector of the U.S. economy. On behalf of the electric power sector, NERC has recognized and responded to this challenge, first through a voluntary cybersecurity standard and now through proposed mandatory Critical Infrastructure Protection ("CIP") Reliability Standards for the bulk power grid. These mandatory standards are intended to assure that the electricity industry will devote the necessary organizational resources to securing control systems, and that the industry will identify, respond to and report cyber security incidents related to critical cyber assets.

Since its establishment in 1968, NERC's mission has been the development and implementation of standards to ensure the reliable operation of the interconnected North American bulk power electric grid in the U.S. and Canada and Mexico. The system of voluntary standards administered by NERC for more than 30 years was replaced on June 18, 2007, with a new set of mandatory Reliability Standards applicable to all users, owners and operators of the "bulk power system." NERC stands ready to take additional steps as warranted to protect the reliability and cybersecurity of the grid.

Mandatory and enforceable Reliability Standards under Section 215 of the FPA are to provide for the reliable operation of the bulk power system only. Section 215 expressly excludes local distribution facilities from the definition of "bulk power system." Moreover, Section 215 does not extend any authority for the regulation of reliability or cybersecurity beyond that which is necessary for reliable operations of the transmission grid. While critical infrastructures in various sectors of the U.S. economy are dependent upon the bulk power system, NERC's authority to propose and enforce reliability standards is confined to a single sector of the economy.

---

[1] NERC is the corporate successor to the North American Electric Reliability Council, also called "NERC," formed to serve as the electric reliability organization ("ERO") authorized by Section 215 of the FPA.

[2] Energy Policy Act of 2005, Pub. L. No. 109-58, Title XII, Subtitle A, 119 Stat. 594, 941 (2005).

We will evaluate how all of our Reliability Standards work in practice, monitor industry and technology developments, and determine on an ongoing basis whether these Standards should be improved, or new standards should be promulgated. The key to improving the reliability of the North American bulk power system is to put in place good standards, as soon as possible. The CIP Reliability Standards are a sound starting point for the electric industry. They can and should be made effective promptly so that they can be implemented now.

In the course of developing the CIP Reliability Standards, NERC evaluated the National Institute of Standards and Technology's ("NIST") ongoing work to apply its Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems, to control systems, and other work underway at NIST to develop guidance on securing control systems. However, the need for mandatory cybersecurity standards to secure grid reliability is immediate, and issuance of the CIP Reliability Standards could not be delayed in order to await completion of the NIST process.

Importantly, bulk power system reliability standards also must be acceptable to regulators in Canada and Mexico. We are not addressing only U.S. facilities with these standards. The NERC standards development process provides a carefully crafted mechanism designed to ensure that final standards proposals have been developed with Canadian (and Mexican, where appropriate) input. Because the NIST guideline development process does not have to take into account the international aspect of the bulk power grid, the U.S. government standards for U.S. government facilities resulting from that process would not necessarily be acceptable.

Moreover, there are also important substantive and process-related reasons why any future final NIST guidelines cannot substitute for Reliability Standards developed specifically for the bulk power grid. First, the guidelines available from NIST for information security when the CIP Reliability Standards were being developed were not appropriate for control systems. Second, Section 215 of the FPA sets forth requirements for the process and procedures through which NERC, as the ERO, may establish Reliability Standards. FERC has approved the NERC standards-setting process. The conversion of a NIST guideline developed for information systems directly into a mandatory Reliability Standard for electric grid control systems would not comply with the statutory procedural requirements under which NERC operates.

NERC will continue to monitor the progress of the NIST process, and as CIP Reliability Standards continue to evolve, there will be future opportunities to continue to reflect NIST documents and guidance as appropriate.

I. BACKGROUND

A. NERC.

NERC's mission is to ensure the bulk power system in North America is reliable. To achieve this objective, NERC develops and enforces reliability standards; monitors the bulk power system; assesses and reports on future adequacy; evaluates owners, operators, and users for reliability preparedness; and educates, trains and certifies industry personnel. NERC is a self-regulatory organization that relies on the diverse and collective expertise of industry

participants. FERC certified NERC as the electric reliability organization ("ERO") in July 2006.[3]

Because Reliability Standards are applicable to the entire, interconnected North American bulk power system, NERC is subject to oversight by the governmental authorities in both Canada and the United States. In the U.S., with oversight from FERC, as of June 18, 2007, NERC has legal authority to enforce reliability standards applicable to all owners, operators, and users of the bulk power system, rather than relying on voluntary compliance. NERC is seeking similar recognition by governmental authorities in Canada, including eight provinces and the National Energy Board, and will seek recognition in Mexico at the appropriate time.

B. Statutory Authority Over Bulk Power System Reliability.

Section 215 of the Federal Power Act establishes the framework for mandatory and enforceable Reliability Standards applicable to all users, owners and operators of the bulk power system. Section 215 assigns to the Commission the duties of approving and enforcing rules to ensure the reliability of the Nation's bulk power system. Section 215 requires the Commission to issue rules for the certification of an ERO charged with developing and enforcing mandatory Reliability Standards, subject to Commission approval. Section 215 also gives the Commission the regulatory responsibility to approve standards that protect the reliability of the bulk power system.

Consistent with the law, the development and enforcement of Reliability Standards is now the responsibility of the ERO. As noted above, FERC's certification of NERC as the ERO places this responsibility squarely on NERC. However, NERC's authority pursuant to Section 215 relates solely to ensuring the reliability of the bulk power system. FPA Section 215(a)(1) defines the term "bulk power system" to mean

> (A) facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and
> (B) electric energy from generation facilities needed to maintain transmission system reliability.

The statutory definition expressly excludes "facilities used in the local distribution of electric energy."

FPA Section 215 defines the term "Reliability Standard" to mean:

> a requirement, approved by the Commission . . . to provide for reliable operation of the bulk-power system. The term includes requirements for the operation of existing bulk-power system facilities, including cybersecurity protection, and the design of planned additions or modifications to such facilities to the extent necessary to provide for reliable operation of the bulk-power system, but the term does not include any requirement to enlarge such facilities or to construct new transmission capacity or generation capacity.

---

[3] *See Order Certifying North American Electric Reliability Corporation as the Electric Reliability Organization and Ordering Compliance Filing*, 116 FERC ¶ 61,062 (2006).

FPA Section 215(a)(3). Under FPA Section 215(a)(4), "reliable operation," as used in the definition of Reliability Standard, means

> operating the elements of the bulk-power system within equipment and electric system thermal, voltage and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements.

The statute also defines a "cybersecurity incident" that the Reliability Standards developed by the ERO are to guard against:

> "cybersecurity incident" means a malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of those programmable electronic devices and communication networks including hardware, software and data that are essential *to the reliable operation of the bulk power system.*

FPA Section 215(a)(8) (emphasis supplied).

Congress spent eight years considering the need for reliability legislation and refining the legislative language, choosing its words carefully to be very specific about the extent of and limitations on the jurisdiction of FERC and the ERO with respect to enforceable reliability standards. Congress also was clear that it wanted to capture the expertise of the industry in developing Reliability Standards and in monitoring and enforcing compliance with Standards through an audited self-regulatory system. For this reason, and because Reliability Standards apply not only in the U.S. but also in Canada, FERC's role is one of approving standards, not developing them in the first place, and in overseeing the activities of the ERO. FPA Section 215(d)(2) provides that in executing its responsibilities to review, approve and enforce mandatory reliability standards, the Commission is authorized to approve those proposed standards that the Commission finds are just, reasonable, not unduly discriminatory or preferential, and in the public interest. Moreover, the Commission "shall give due weight to the technical expertise of the Electric Reliability Organization with respect to the content of a proposed reliability standard. . . ." Further, the statute requires that in applying its expertise and developing Reliability Standards, the ERO certified by the Commission must have established rules that "provide for reasonable notice and opportunity for public comment, due process, openness, and balance of interests in developing reliability standards . . . ." *See* FPA section 215(c)(2)(D).

II. RESPONSE TO ISSUES IDENTIFIED BY THE COMMITTEE

A. NERC's Authority To Prescribe Critical Infrastructure Protection Rules Is Limited To The Electric Power Sector Only And Does Not Extend To Regulation Of Distribution Systems Or Other Infrastructures.

As described above, the authority granted to the ERO pursuant to Section 215 of the Federal Power Act is not unlimited. FPA Section 215 does not convey authority to apply mandatory and enforceable reliability standards to the distribution system. The authority of the ERO extends only to elements of the bulk power system as defined in the statute. The only entities that under the law must comply with ERO-developed reliability standards are "users, owners and operators of the bulk-power system." Subject to FERC's approval, NERC has developed a compliance registry that identifies these entities, consistent with the statutory requirements.

The standards that NERC has proposed to the Commission are consistent with Section 215 of the FPA. We believe those standards, when taken as a whole and as they develop over time, will continue to provide a level of reliability that is commensurate with the statutory requirements.

B. The CIP Reliability Standards Were Developed Through A Rigorous Process That Took The NIST Guidance Into Account.

Section 39.5(a) of the Commission's regulations requires the ERO to file with the Commission for approval each reliability standard the ERO proposes to become mandatory and enforceable in the United States, and each proposed modification to a reliability standard. NERC and the Commission have made substantial progress in proposing and approving reliability standards to be mandatory and enforceable in the United States. NERC filed a petition for approval of 102 existing Reliability Standards in FERC Docket No. RM06-16 on April 4, 2006. NERC filed a second petition for the approval of proposed reliability standards August 28, 2006, submitting 16 new standards for approval and revisions to 11 of the reliability standards previously submitted. Of the 16 new standards submitted, eight were Critical Infrastructure Protection cyber security standards.

On December 11, 2006, the Commission Staff issued an assessment of the cyber security standards as a basis to solicit comments on those proposed standards. On July 20, 2007, the Commission issued a Notice of Proposed Rulemaking ("NOPR") generally proposing to approve the CIP Reliability Standards as mandatory and enforceable, while also proposing to require NERC to make specific modifications to certain of the standards.[4] The deadline for comments

[4] *Mandatory Reliability Standards for Critical Infrastructure Protection*, Docket No. RM06-22, 120 FERC ¶ 61,077 (2007). FERC's NOPR described the proposed CIP Reliability Standards as "the most thorough attempt to date to address cyber security issues that relate to the Bulk-Power System." NOPR, P 13. Given the nature of the cyber security threat, the Commission acknowledged that "cyber security strategies must comprise a layered, interwoven approach to vigilantly protect the Bulk-Power System against evolving cyber security threats." NOPR, P 15. FERC proposed to approve NERC's proposed Implementation Plan for the CIP Reliability Standards, which sets forth "a timeline by calendar quarters for completing various tasks and prescribes milestones for when a responsible entity

on the NOPR was October 5, 2007, and the Commission has received approximately 100 comments on the staff assessment and the proposed standards.

1. Background of Proposed Cyber Security Standards.

The initial work on the proposed cyber security standards dates back to 2002 when NERC's Critical Infrastructure Protection Advisory Group ("CIPAG")[5] drafted cyber security language that ultimately appeared in Appendix G of the Commission's "Standard Market Design" NOPR.[6] Since then, NERC has continued to raise the bar on cyber security, first by adopting Cyber Security Urgent Action Standard 1200 in 2003,[7] and again with the proposed standards filed with the Commission in August 2006.

Reflecting Congress's objective in FPA Section 215 that industry expertise should be brought to bear in the development of Reliability Standards, the proposed cyber security standards have been crafted with significant industry input by experts in the area and a debate of key issues through a process accredited by the American National Standards Institute ("ANSI"). The Standard Authorization Request ("SAR") for the cyber security standards was submitted to NERC on May 2, 2003. After two public comment periods, the industry reached a consensus on the scope and justification for the standards. The Standards Authorization Committee ("SAC") appointed a drafting team of security experts to begin development of these standards in May 2004.

Drafting team members brought significant experience and expertise from a broad spectrum of security related disciplines including information technology security, physical security, compliance auditing, personnel and training, energy management systems ("EMS"), and system control and data acquisition ("SCADA") system operations. Drafting team members also brought expert knowledge of existing government regulations affecting security such as Sarbanes-Oxley and the Federal Information Security Management Act of 2002 ("FISMA"), as well as existing security related standards such as International Standards Organization ("ISO") Standard 17799 and the body of work promulgated by NIST. A number of members of the

---

must: (1) "begin work;" (2) "be substantially compliant" with a requirement; (3) "be compliant" with a requirement; and (4) "be auditably compliant" with a requirement." NOPR, PP 43,47. FERC also proposed to approve the 162 proposed Violation Risk Factor assignments proposed by NERC that correspond to the requirements of the CIP Reliability Standards and to direct NERC to revise 43 of them, as well as to assign Violation Risk Factors to additional requirements under the CIP Reliability Standards. NOPR, P 325. Violation Risk Factors indicate the potential or expected impact to the reliability of the Bulk-Power System of the violation of a particular Reliability Standard requirement. Violation Risk Factors are used by NERC in setting penalty amounts for violations of a Reliability Standard.

[5] The CIPAG was a predecessor organization to NERC's current Critical Infrastructure Protection Committee ("CIPC").

[6] *Remedying Undue Discrimination through Open Access Transmission Service and Standard Electricity Market Design, Notice of Proposed Rulemaking*, 67 Fed. Reg. 55,452 (Aug. 29, 2002), FERC Stats. & Regs. ¶ 32,563 (2002). The Standard Market Design NOPR was never finalized.

[7] Cyber Security Urgent Action Standard 1200 was a voluntary standard that applied to control areas, transmission owners and operators, and generation owners and operators performing certain specific functions. The voluntary standard established a self-certification process relating to the security of system control centers of covered entities. The Urgent Action 1200 standard was effective on a voluntary basis until June 1, 2006, when it was replaced by the eight CIP Reliability Standards that are the subject of the current FERC rulemaking.

drafting team held professional security certifications. Membership on the drafting team fairly represented ownership segments in the electric industry and a balance between U.S. and Canadian participation.

Throughout the development process, the drafting team insisted on looking beyond generally accepted "best practices." They sought to establish relevant, thorough requirements with unambiguous measures for determining compliance. Three versions of the cyber security standards were posted to solicit input from the industry and other interested parties. More than 2,500 pages of comments and responses to the comments were provided in response to the three postings of the draft standards. The fourth and final version was submitted to ballot of the stakeholders. The number and volume of comments received represented an extraordinary level of involvement by the industry during the development process.

2. NERC's CIP Reliability Standards Proposal.

In the August 2006 submission to FERC, NERC proposed eight new cybersecurity standards (CIP-002-1 to CIP-009-1) to provide a comprehensive set of requirements to protect the bulk power system from malicious cyber attacks. Because there are unique aspects of cyber protection for each entity and its assets, the standards require bulk power system owners, operators, and users to step through a sequence of establishing a risk-based vulnerability assessment method and using that method to identify and prioritize critical assets and critical cyber assets. Once the critical cyber assets are identified, the standards require the responsible entities to establish plans, protocols, and controls to safeguard physical and electronic access, to train personnel on security matters, to report security incidents, and to be prepared for recovery actions. The proposed cyber security standards propose the most comprehensive set of requirements ever utilized on a widespread basis in the electric industry.

Because of the expanded scope of facilities and entities covered by these standards, and the investment in security upgrades required in many cases, the implementation plan calls for a three-year phase-in to achieve full compliance with all requirements. The transition builds progressively from the requirements that were previously in place with the 1200 Urgent Action Standard. In other words, the industry is improving its security measures in stages from the level established in 2003 with the interim standard to an extraordinarily robust set of auditable requirements by end of year 2009.

The proposed standards will apply to 11 categories of "Responsible Entities," including NERC itself, the Regional Reliability Entities, reliability coordinators [which may include Regional Transmission Organizations or Independent System Operators], balancing authorities, interchange authorities, transmission service providers, transmission owners, transmission operators, generator owners, generator operators, and load serving entities. As set forth in the NOPR, the proposed standards address:

- **CIP-002-1 – Cyber Security – Critical Cyber Asset Identification**:
  Requires a responsible entity to identify its critical assets and critical cyber assets using a risk-based assessment methodology.

- **CIP-003-1 – Cyber Security – Security Management Controls**:
  Requires a responsible entity to develop and implement security management controls to protect critical cyber assets identified pursuant to CIP-002-1.

- **CIP-004-1 – Cyber Security – Personnel & Training**:
  Requires personnel with access to critical cyber assets to have an identity verification and a criminal check. Also requires employee training.

- **CIP-005-1 – Cyber Security – Electronic Security Perimeters**:
  Requires the identification and protection of an electronic security perimeter and access points. The electronic security perimeter is to encompass the critical cyber assets identified pursuant to the risk-based assessment methodology required by CIP-002-1.

- **CIP-006-1 – Cyber Security – Physical Security of Critical Cyber Assets**:
  Requires a responsible entity to create and maintain a physical security plan that ensures that all cyber assets within an electronic security perimeter are kept in an identified physical security perimeter.

- **CIP-007-1 – Cyber Security – Systems Security Management**:
  Requires a responsible entity to define methods, processes, and procedures for securing the systems identified as critical cyber assets, as well as the non-critical cyber assets within an electronic security perimeter.

- **CIP-008-1 – Cyber Security – Incident Reporting and Response Planning**:
  Requires a responsible entity to identify, classify, respond to, and report cyber security incidents related to critical cyber assets.

- **CIP-009-1 – Cyber Security – Recovery Plans for Critical Cyber Assets**:
  Requires the establishment of recovery plans for critical cyber assets using established business continuity and disaster recovery techniques and practices.

The cyber security standards proposed by NERC provide firm requirements that can be implemented by all participants in the electricity sector regardless of size, staffing levels, or levels of sophistication. Some members of the electricity sector already meet or exceed the proposed standards. However, the standards may be a significant burden on some entities that have not heretofore been required to implement cyber security programs. Throughout the development process, the drafting team attempted to push the bar beyond the generally accepted industry best practices, and to ensure that every component part has at least the minimum protection necessary to protect the reliability of the bulk power system as a whole. The resulting standards represent a balanced set of outcomes in a diverse industry. These standards are rigorous, but compliance can be achieved by all "owners, operators and users" of the bulk power system.

The proposed cyber security standards fulfill relevant portions of Recommendations 32 and 32.A of the *United States/Canada Power System Outage Task Force* report. These recommendations state, in part, that NERC should finalize and implement the CIP-002-1 to CIP-

009-1 standards, that NERC standards related to physical and cyber security should be made mandatory and enforceable, and that NERC should take actions to better communicate and enforce these standards. To help the industry understand and implement these standards, NERC held a series of ten industry workshops on the standards for bulk power system owners, operators, and users that were conducted across North America.

NERC also believes that these cyber security standards are a landmark for the implementation of mandatory cyber security in a non-business environment. These standards represent, for the first time, a set of mandatory security requirements for an entire industry. Other statutory and regulatory attempts have not been as proscriptive or as specific as these standards.

These proposed standards are different from traditional information technology security standards. The CIP Reliability Standards apply information technology security principles, which are commonly accepted in the business environment, to bulk power system control systems which were not designed with these security principles in mind. As such, the security principles must be carefully applied to ensure that there are no unintended consequences that undermine bulk power system reliability. These standards must prescribe what is required of real-time critical bulk power system operating systems. This differs from what can be prescribed for secured business systems.

Promulgating standards for the bulk power system that draw too closely on the standards appropriate for secured business systems could result in a *less reliable* bulk power system, either because of decreased operations or decreased security. Two examples of this are 1) the use of password-protected screen savers on computers, and 2) automatic lockout of accounts following invalid passwords. Both of these are accepted business system security practices, but they lead directly to reduced ability to reliably operate a real-time control system, and thus to a less reliable bulk power system. In the case of a password-protected screensaver, the business justification is to reduce the release of confidential information or misuse of the computing resources; in a control system, it results in a lack of visibility of key real-time operating parameters that must be constantly observed to ensure reliable operations. In the case of password lockout, business systems use the lockout as a preventative measure to ensure that information and computer resources cannot be used following an concerted attack; in a control system the need to rapidly be able to get access to a system under all circumstances may result in mis-typed passwords, which could lead to the complete inability to monitor or take corrective actions to maintain reliable operations. In both cases, control systems implement alternate mitigating controls, including increased physical security and additional personnel that the business systems cannot assume, to ensure that the systems are not misused.

The proposed cyber security standards will increase the reliability of the bulk power system by improving the resiliency of the control system cyber assets and improving their ability to withstand cyber-based attacks. Cyber security requirements will be applied to functions and companies where they have never before been applied. NERC has applied cyber security standards to control centers through prior standards; however, the Standards currently before the Commission are the first to require cyber security in either a substation or generating plant environment.

3. Interaction Between NERC and NIST Processes.

The FERC NOPR addresses the relationship between the CIP Reliability Standards and other existing standards for cyber security, both governmental standards and industrial standards. *See* NOPR, PP 87-88. Specifically, the Commission received a recommendation that Federal Information Processing Standards ("FIPS") 199, FIPS 200, and NIST Special Publication 800-53 Revision 1, Recommended Security Controls for Federal Information Systems ("SP 800-53") be used as the basis for cyber security requirements applicable to the electric power sector. The National Institute of Standards and Technology recommended that FERC consider a transition to cyber security standards identical to, consistent with or based on SP 800-53 and related guidelines.

The Commission declined to propose such a transition in the NOPR:

> The Commission declines to propose at this time that NERC incorporate any provisions of the NIST standards into the CIP Reliability Standards. However, the Commission expects NERC to monitor the development and implementation of the NIST standards to determine if they contain provisions that will better protect the Bulk-Power System. Several federal entities, such as the Tennessee Valley Authority and Western Area Power Administration, are subject to both the NIST standards and the Reliability Standards, and therefore are likely to have unique insights into the NIST standards. The Commission expects the ERO to seek and consider comments from those federal entities on the effectiveness of the NIST standards and on any implementation issues. Any provisions that will better protect the Bulk-Power System should be addressed in the ERO's Reliability Standards development process. The Commission may revisit this issue in future proceedings as part of an evaluation of existing Reliability Standards or the need for new Reliability Standards, or as part of assessing NERC's performance of its responsibilities as the ERO.

NOPR, P 88 (footnote omitted).

NERC agrees fully with the Commission's determination. During the development of the CIP Reliability Standards discussed above, participants in the standards development process acknowledged that NIST's existing FISMA guidance is not appropriate for control systems. NIST has continued its work in this area, and has developed guidance, which is still in the draft stage, on applicable actions to be performed in support of FISMA compliance to control systems. To date, NIST has released two public draft versions of its revised guidance (in July 2005 and June 2007). As of this date, however, the guidance has not been approved by NIST, nor issued in final form. Given the importance of the cybersecurity standards and the critical need to have standards in place and enforceable as soon as possible, it would not have been appropriate to delay the NERC standards development process in order to await the final outcome of the NIST process.

Additionally, as described above, NERC's procedures for the development of reliability standards are governed by the Federal Power Act. In certifying NERC as the ERO, FERC approved NERC's ANSI-approved standards development process as consistent with the

statutory requirements. This ANSI-approved process is essentially the same as that used by other standards organizations, including the IEEE, ISA, and ANSI itself. In contrast, the NIST process is not an ANSI-accredited process, and does not include a stakeholder ballot. As all of the Reliability Standards developed by NERC and submitted to FERC for approval must be developed through the FERC-approved ANSI process, NERC cannot simply adopt a NIST guideline as a Reliability Standard. While the NIST proposals can be (and have been) considered in the ERO standards development process, the resulting standard cannot be the NIST document or guideline.

C. While Interdependency Is A Significant Issue, The CIP Reliability Standards Can Only Address Critical Assets In The Electricity Sector.

Another issue addressed in the NOPR, and in the FERC staff assessment proposed CIP-002-1 regarding the identification of critical assets, concerned the "interdependency" with other infrastructures. The staff assessment asked for comments on whether CIP-002-1 should address this matter, and whether there should be coordination and collaboration in the future with other industries and government agencies. In the NOPR, FERC concluded that:

> While broader interdependency issues cannot be ignored, the Commission intends to revisit this matter through future proceedings and with other agencies. This work will help to inform the electric sector and this Commission about the need for future Reliability Standards, especially when the interdependent infrastructures affect generating capabilities, such as through fuel transportation.

NOPR, P 118.

NERC concurs that the interdependency issue raised in the NOPR is an important one; however, the issue is too broad to be restricted to a single agency or industry sector. We believe that it is best raised through direct cooperation with other critical infrastructure sectors through existing cross-sector initiatives such as the Partnership for Critical Infrastructure Security ("PCIS") and the Information Sharing and Analysis Center Council ("ISAC Council"), with the lead federal government agency being the U.S. Department of Homeland Security. Once specific issues directly relating to the reliability of the bulk-power system are identified through these organizations, standards creation activities can be initiated through the ERO to address them.

III. CONCLUSION

The approval by FERC of the proposed CIP Reliability Standards will represent an important milestone in the transition to the system of mandatory and enforceable reliability standards envisioned by Congress in the Energy Policy Act of 2005, that will ensure grid reliability by improving the resiliency of the control system cyber assets and improving their ability to withstand cyber-based attacks.

Going forward, standards development requires progressive and continuous improvement. NERC's rules, and a condition of accreditation by the American National Standards Institute, require that each standard be reviewed at least every five years. NERC

anticipates completing the review and upgrade of all standards over a three-year period, beginning with the highest priority standards in 2007. NERC's standards development procedure provides a systematic approach to improving to the standards and documenting the basis for those improvements, and should serve as the mechanism for achieving those improvements.

These CIP Reliability Standards already represent a significant improvement of cyber security for the electricity industry. Since our process requires that standards be continuously improved, the standards will be reviewed, modified and improved by necessity of the process. This will result in an ever-increasing improvement to the level of cyber security throughout the electricity industry. However, the process must start somewhere with a set of standards. Based on NERC's development process, and the demonstrated broad base of support, the standards currently before the Commission represent the most appropriate starting point for today's environment.

David A. Whiteley
Executive Vice President
North American Electric Reliability Corporation
116-390 Village Boulevard
Princeton, New Jersey 08540-5721
609-452-8060

SUMMARY:

Mandatory and enforceable Reliability Standards under Section 215 of the Federal Power Act are to provide for the reliable operation of the bulk power system only. Section 215 does not extend any authority for the regulation of reliability or cybersecurity beyond that which is necessary for reliable operations of the transmission grid. While critical infrastructures in various sectors of the U.S. economy are dependent upon the bulk power system, NERC's authority to propose and enforce reliability standards is confined to a single sector of the economy.

NERC will evaluate how all of Reliability Standards work in practice, monitor industry and technology developments, and determine on an ongoing basis whether these Standards should be improved, or new standards should be promulgated. The key to improving the reliability of the North American bulk power system is to put in place good standards, as soon as possible. The CIP Reliability Standards are a sound starting point for the electric industry. They can and should be made effective promptly so that they can be implemented now.

In the course of developing the CIP Reliability Standards, NERC evaluated NIST's ongoing work to apply its Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems, to control systems, and other work underway at NIST to develop guidance on securing control systems. The guidelines available from NIST for information security when the CIP Reliability Standards were being developed were not appropriate for control systems. Moreover, Section 215 of the FPA sets forth requirements for the process and procedures through which NERC, as the ERO, may establish Reliability Standards. The conversion of a NIST guideline developed for information systems directly into a mandatory Reliability Standard for electric grid control systems would not comply with the statutory procedural requirements under which NERC operates. Because of the pressing need for mandatory cybersecurity standards to secure grid reliability, issuance of the CIP Reliability Standards could not be delayed in order to await completion of the NIST process. NERC will continue to monitor the progress of the NIST process, and as CIP Reliability Standards continue to evolve, there will be future opportunities to continue to reflect NIST documents and guidance as appropriate.

DISCLOSURE REQUIREMENT
Required by House Rule XI, clause 2(g)

1. Name: David A. Whiteley

2. Business Address: 116-390 Village Boulevard
Princeton, New Jersey 08540

3. Organization you are representing: North American Electric Reliability Corporation (NERC)

4. Any federal grants or contracts (including subgrants or subcontracts) which **you, personally,** have received since October 1, 2005, from Federal Agencies under the purview of the hearing, the source and the amount of each grant or contract:

None

5. Any federal grants or contracts (including subgrants or subcontracts) which were received since October 1, 2005, from Federal Agencies under the purview of the hearing by the **organization(s) which you represent** at this hearing, including the source and amount of each grant or contract:

None